

Serial No.: 10/527,235
Attorney Docket No.: 039996-7
Page 2 of 5

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1-16. (Canceled).

17. (Currently Amended) ~~The method of claim 1 further including~~ A method for securing a computer system that includes one or more mobile devices and a computing node, comprising:

executing a node security program in the computing node for interpreting a node security profile;

determining at least one security parameter from the interpretation of the node security profile;

managing at least one security process between the computing node and one or more mobile devices based on the at least one security parameter determined by interpreting the node security profile, and

transferring a device security profile to a mobile device or a resource device to be interpreted by a device security program running on the mobile device to determine device security parameters.

18. (Original) The method of claim 17, wherein transferring the device security profile comprises accessing at least one of a server station, a central station, and a computing node or a website.

19. (Original) The method of claim 17, wherein the device security profile is transferred based on at least one of a temporal attribute and a position of the mobile device in at least one of real time or non-real time modes.

20. (Original) The method of claim 17 further comprising periodically updating at least one of the node security profile and device security profile.

W704882.1

Serial No.: 10/527,235
Attorney Docket No.: 039996-7
Page 3 of 5

21. (Currently Amended) The method of claim 17, wherein the step of transferring includes at least one of a data synchronization process, data transfer, file transfer, and an email between the computing node and a mobile device or[[e]] resource.

22-25. (Canceled).

26. (Original) The method of claim 17 further including transmitting at least one of the node security profile and device security profile using at least one of a push or pull technology.

27. (Original) The method of claim 17 further including transmitting at least one of the node security profile and device security profile using an over the air protocol.

28-32. (Canceled).

33. (Original) A method for managing a computer system including a computing node and one or more mobile devices, comprising:

running a discovery program to detect one or more mobile devices or resources;

determining information regarding one or more mobile devices or resources based on at least one of a registry resource, a file resource, a process resource, a network management parameter, a data format, a packet format, a synchronization log entry, a directory structure, a database entry, the presence of an executable program and attributes associated with a mobile device or resource; and

using the determined mobile device information for managing security of the computer system.

34. (Original) The method of claim 33 further including scanning the computer system based on a scan profile to detect the one or more mobile devices.

w704882.1

Serial No.: 10/527,235
Attorney Docket No.: 039996-7
Page 4 of 5

35. (Original) The method of claim 33, wherein the discovery program is run in at least one of a remote central station or a local computing node.

36. (Original) The method of claim 33 further including grouping the located mobile devices or resources by type and other attribute.

37. (Original) The method of claim 33, wherein the scan profile contains information regarding at least one of network, domain, IP address, netmask, and computer identity to be scanned, time of synchronization and device connection.

38. (Original) The method of claim 33, wherein the scan profile contains information regarding at least one of network, domain, IP address, netmask, and computer identity not to be scanned.

39. (Original) The method of claim 33, wherein the results of scanning are analyses and populated and stored and displayed to the users.

40. (Original) The method of claim 33, wherein the gather mobile device information include at least one of device type, device identity, synchronization software type, synchronization software availability, synchronization software location, synchronization software version number, previous synchronization information, data and time of last synchronization, the type of device used during previous synchronization, synchronization ID, device owner information, type of applications and files installed or used on the mobile device, file size, file name, file attribute, manufacturer information, time of all completed and incomplete synchronization and data access and connections performed, type of data and information transferred to and from a mobile device and a resource.

W704882.1